⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3－189756

⑤1Int. Cl.⁵	識別記号	庁内整理番号
G 06 F 15/00	330 F	7218－5B
15/62	455	9071－5B
G 09 C 1/00		7343－5B

⑬公開　平成3年(1991)8月19日

審査請求　未請求　請求項の数 1　（全8頁）

⑤4発明の名称　コンピュータ装置の使用者確認装置

⑳特　願　平1－330488

㉒出　願　平1(1989)12月19日

⑦2発明者　川崎　孝二　愛知県刈谷市昭和町1丁目1番地　日本電装株式会社内

⑦2発明者　神谷　敏玄　愛知県刈谷市昭和町1丁目1番地　日本電装株式会社内

⑦2発明者　鈴木　隆夫　愛知県刈谷市昭和町1丁目1番地　日本電装株式会社内

⑦1出願人　日本電装株式会社　愛知県刈谷市昭和町1丁目1番地

⑦4代理人　弁理士　藤谷　修

明　細　書

1. 発明の名称

コンピュータ装置の使用者確認装置

2. 特許請求の範囲

コンピュータ装置の使用が許可されている使用者の指紋画像データを予め登録指紋画像データとして記憶しておき、そのコンピュータ装置の使用時に使用者の指紋を読み取り、その使用者の入力指紋画像データを作成し、その入力指紋画像データと前記登録指紋画像データとを照合し、その照合結果に応じてコンピュータ装置の許可された使用者を確認する使用者確認装置において、

使用者の指紋を読み取り、2値化された指紋画像データを生成する指紋画像データ生成手段と、

登録すべき使用者の指紋に対して、前記指紋画像データ生成手段により得られた指紋画像データを暗号化する暗号化手段と、

前記暗号化手段により暗号化された暗号化登録指紋画像データを記憶する前記コンピュータ装置の外部記憶装置と、

前記暗号化登録指紋画像データを復号するための解読鍵データを記憶し、前記コンピュータ装置から読み書き不可能な第1記憶手段と、

前記コンピュータ装置から読み取り可能な第2記憶手段と、

指紋の照合時には前記第1記憶手段に記憶された解読鍵データを前記第2記憶手段に転送するデータ転送手段と、

指紋の照合時には前記外部記憶装置に登録された前記暗号化登録指紋画像データを読み取り、その暗号化登録指紋画像データを前記第2記憶手段に記憶された解読鍵データに基づいて復号化する復号化手段と、

前記復号化手段により復合化された登録指紋画像データと、前記指紋画像データ生成手段により得られた使用者の前記入力指紋画像データとを照合する照合手段と、

を有することを特徴とするコンピュータ装置の使用者確認装置。

3. 発明の詳細な説明

【産業上の利用分野】

本発明はコンピュータ装置の使用者が登録された使用者か否かを確認するための使用者確認装置に関する。

【従来技術】

従来、コンピュータ装置の使用者の本人確認を行う方法として、パスワードやＩＤコードの照合を行う方法が知られている。更に、本人確認をより完全なものとする方法として、コンピュータの使用時に、使用者の指紋を読み取り、その入力指紋画像データと予め登録された登録指紋画像データとを照合して、その照合結果に応じて、本人確認を行う方法が知られており、そのための指紋照合装置も知られている。

【発明が解決しようとする課題】

しかし、このような指紋照合装置では、登録指紋画像データは、指紋照合装置の内部のメモリＩＣに記憶される。従って、登録される使用者が多くなると、メモリの容量が増大し、指紋照合装置が大型化するという問題がある。この問題点を解決するために登録指紋画像データをコンピュータ装置の記憶容量の大きな外部記憶装置等に格納すると、容易にその登録指紋画像データが読み取られるという機密保持上の問題がある。

本発明は上記課題を解決するために成されたものであり、その目的は、機密保持の行われた小形化された指紋照合装置を提供することである。

【課題を解決するための手段】

上記課題を解決するための発明の構成は、第１図にその概要を示すように、使用者の指紋を読み取り、２値化された指紋画像データを生成する指紋画像データ生成手段A1と、登録すべき使用者の指紋に対して、指紋画像データ生成手段A1により得られた指紋画像データを暗号化する暗号化手段A2と、暗号化手段A2により暗号化された暗号化登録指紋画像データを記憶するコンピュータ装置の外部記憶装置A3と、暗号化登録指紋画像データを復号するための解読鍵データを記憶し、コンピュータ装置から読み書き不可能な第１記憶手段A4と、コンピュータ装置から読み取り可能な第２記憶手段A5と、指紋の照合時には第１記憶手段A4に記憶された解読鍵データを第２記憶手段A5に転送するデータ転送手段A6と、指紋の照合時には外部記憶装置A3に登録された暗号化登録指紋画像データを読み取り、その暗号化登録指紋画像データを第２記憶手段A5に記憶された解読鍵データに基づいて復号化する復号化手段A7と、復号化手段A7により復合化された登録指紋画像データと、指紋画像データ生成手段A1により得られた使用者の指紋画像データとを照合する照合手段A8とを設けたことである。

【作用】

使用者登録において、コンピュータ装置の使用者の指紋は、指紋画像データ生成手段A1により読み取られ、２値化された指紋画像データが生成される。その指紋画像データは、暗号化手段A2により暗号化されて、ハードディスク装置やフロッピィディスク装置等のコンピュータの外部記憶装置A3に記憶される。又、外部記憶装置A3に記憶された暗号化指紋画像データを復号化するための解読鍵データは、コンピュータ装置から読み書き不可能な第１記憶手段A4に記憶されている。従って、コンピュータ装置の一般の利用者は、外部記憶装置A3に記憶された登録指紋画像データを判読することができない。

コンピュータ装置を使用する場合には、使用者の読み取られた指紋画像データと登録指紋画像データとの照合が行われ、両者が一致すれば、コンピュータ装置の使用が許可される。

指紋照合時において、コンピュータ装置の使用者の指紋は、指紋画像データ生成手段A1により読み取られ、２値化された指紋画像データが生成される。又、データ転送手段A6により第１記憶手段A4に記憶された解読鍵データが第２記憶手段A5に転送される。そして、復号化手段A7により、外部記憶装置A3に記憶された暗号化登録指紋画像データが読み取られ、その暗号化登録指紋画像データは、第２記憶手段A5に一時的に記憶された解読鍵データに基づいて、復号される。次に、使用者の入力された指紋画像データと復号化された登録指

紋画像データとが、照合手段A8により照合され、その照合結果に応じて、コンピュータ装置の使用者が登録された使用者か否かの判定が行われる。この判定結果により、これからコンピュータ装置を使用しようとする者が登録された使用者と確認された場合には、そのコンピュータ装置の使用が許可され、そうでない場合には、コンピュータ装置の使用が禁止される。

【実施例】

以下、本発明を具体的な実施例に基づいて説明する。

第２図は、本実施例に係るコンピュータ装置の使用者確認装置を示した斜視図である。１０はパーソナルコンピュータ装置本体、３０はCRT ディスプレイ、５０はコンピュータ装置の使用者の指の指紋を検出する指紋画像入力装置、９０はキーボードである。又、コンピュータ装置本体１０には、外部記憶装置としての２台のフロッピィディスク装置１１と、画像データを処理する画像処理装置７０が設けられている。

第３図は、上記装置の電気的構成を示したブロック図である。

中央処理装置（以下「CPU 」と記す）１２には、入出力インタフェース１３を介して外部記憶装置としてのフロピィディスク装置１１が接続されており、そのフロッピィディスク装置１１には、暗号化された登録指紋画像データ（以下、「暗号化登録指紋画像データ」という）や、ＯＳ、他のユーザーズプログラム等の記憶されたフロッピィディスク１４が挿着される。又、CPU １２には、データバス、アドレスバス、制御バス等で構成されるバス１５を介して、RAM １６と第２記憶装置としてのRAM ７３が接続されている。更に、CPU １２には入出力インタフェース１８を介してCRT ディスプレイ３０が、入出力インタフェース２０を介してコンピュータ装置に対する指令やデータを入力するためのキーボード９０が接続されている。

一方、画像処理装置７０は、画像処理プロセッサ７１、第１記憶装置としてのRAM ７２、第２記憶装置としてのRAM ７３、指紋画像入力装置５０の接続されるアナログインタフェース７４とを有している。画像処理プロセッサ７１は、指紋画像入力装置５０の出力する指紋画像の映像信号を入力して画素毎に２値化した指紋画像データを生成したり、２つの指紋画像データを画素毎に照合して、一致する画素数を演算したり、指紋画像データを画素単位で順次変位（画像データの平行移動及び回転）させたり、指紋画像データを拡大、縮小させたり、第１記憶装置のRAM ７２と第２記憶装置のRAM ７３との間で指定されたアドレスのデータを指定されたアドレスに転送する機能を有している。そして、画像処理プロセッサ７１は、コンピュータ装置本体１０のバス１５に接続されており、CPU １２の指令語に応じて、上記の機能を選択的に実行することが可能になっている。又、画像処理プロセッサ７１は第１記憶装置としてのRAM ７２と独自の画像バス７５によって接続されているので、画像処理プロセッサ７１は第１記憶装置のRAM ７２と第２記憶装置のRAM ７３との両者をアクセスすることが可能である。それに対し、第１記憶装置７２はバス１５に接続されていないので、CPU １２は、第１記憶装置のRAM ７２を直接、アクセスすることができない。

第１記憶装置としてのRAM ７２には、コンピュータ装置の登録された使用者のＩＤ番号、フロッピィディスク１４に記憶された暗号化指紋画像データを解読するための暗号解読キーデータ、例えば、ＩＤ番号に対応した暗号変換テーブル等が記憶されている。

指紋画像入力装置５０はCCD 等のイメージスキャナーで構成されており、コンピュータ装置の使用者の指の指紋を読み取り、指紋画像の映像信号をアナログインタフェース７４を介して、画像処理プロセッサ７１に出力する機能を有している。

次に、本装置の作動について、CPU １２の処理手順を示した第４図、第５図、第６図のフローチャートに従って説明する。

(1) 最優先管理者の登録

先ず、コンピュータ装置が設置後に初めて起動される時に、例えば、コンピュータ保守者、コン

ピュータ装置のメイカー等のごく限定された者の手によってのみ、第4図に示すプログラムが実行可能となり、使用者の中から選ばれた最優先管理者の登録が実行される。

ステップ100において、キーボード90から最優先管理者のＩＤコードが入力され、そのＩＤコードは第2記憶装置のRAM 73に記憶される。次に、ステップ102において、指紋画像入力装置50が起動され、指紋画像入力装置50から最優先管理者の指紋画像の映像信号が出力される。その映像信号はアナログインタフェース74を介して、画像処理プロセッサ71に入力される。次のステップ104で、画像処理プロセッサ71が起動されて、その画像処理プロセッサ71により、画素毎に映像信号の濃淡レベルが2値化され、指紋画像データとして、第1記憶装置のRAM 72に記憶される。又、ステップ106にて、RAM 73に記憶されている最優先管理者のＩＤコードが第1記憶装置のRAM 72に記憶される。第1記憶装置のRAM 72はCPU 12からは、直接、アクセスできないので、最優先管理者のＩＤコード及び指紋画像データの機密性が保持される。

尚、最優先管理者の登録プログラムは、登録された最優先管理者や、コンピュータ装置の保守者、コンピュータ装置の設計者等のごく限定された者にしか、起動できないように保護されており、最優先管理者の変更等は、上記の者にしか出来ないようになっている。

⑵ 使用者の登録

コンピュータ装置の使用者の登録は、第5図のフローチャートに従って実行される。

使用者の登録は、上述したように、登録された最優先管理者及び以下に述べる方法で登録される通常管理者の立会いの元でのみ実行することができる。

ステップ200では、キーボード90から入力された管理者（コンピュータ装置の使用者登録を行っている現在の操作者）のＩＤコードが読み取られる。次に、ステップ202にて、画像処理プロセッサ71にデータの転送指令が付与される。これにより、画像処理プロセッサ71は第1記憶装置のRAM 72の所定領域に記憶された最優先管理者のＩＤコードと通常管理者のＩＤコードとその通常管理者の暗号化指紋画像データの解読キーデータが、第2記憶装置のRAM 73の所定領域に転送される。次に、ステップ204において、入力されたＩＤコードと登録された最優先管理者のＩＤコードとが一致するか否かが判定され、一致する場合には、ステップ206へ移行して、指紋画像入力装置50が起動されて、その最優先管理者（コンピュータ装置の現在の操作者）の指紋画像が読み取られる。そして、指紋画像入力装置50で読み取られた指紋画像は、画像処理プロセッサ71によって、画素毎に2値化され、入力指紋画像データとして、第2記憶装置のRAM 73の所定領域に記憶される。

次に、ステップ208において、画像処理プロセッサ71に指令が付与され、第2記憶装置のRAM 73に記憶された入力指紋画像データと第1記憶装置のRAM 72に記憶されている最優先管理者の登録指紋画像データとの間で、画素毎に照合演算が実行される。この時、一致する画素数が一定値を越えるまで、2つの画像データ間で、画像の平行移動、回転、拡大、縮小等の操作が多数回実行される。照合する画素数が一定値を越えると照合演算が停止される。又、照合画素数が一定値を越えない場合には、所定回数の照合演算の後に演算を終了する。そして、ステップ210において、画像処理プロセッサ73の出力する結果に応じて、2つの画像データが一致するか否かが判定される。

ステップ210で、2つの指紋画像データが一致すると判定された場合には、ステップ212以下の指紋画像データの登録手順が実行される。

一方、上記のステップ204で入力ＩＤコードが最優先管理者のＩＤコードと一致しないと判定された場合には、ステップ220へ移行して、入力ＩＤコードが第2記憶装置のRAM 73に第1記憶装置のRAM 72から転送された通常管理者のＩＤコードに一致するか否かが判定される。一致すれば、ステップ222に移行して、ステップ206と同様に

して、指紋画像入力装置５０が起動されて、その通常管理者（コンピュータ装置の現在の操作者）の指紋画像が読み取られる。そして、指紋画像入力装置５０で読み取られた指紋画像は、画像処理プロセッサ７１によって、画素毎に２値化され、入力指紋画像データとして、第２記憶装置のRAM ７３の所定領域に記憶される。

通常管理者の指紋画像データは暗号化されて、フロッピィディスク１４に記憶されているので、ステップ224 において、入力ＩＤコードに対応する通常管理者の暗号化指紋画像データが、フロッピィディスク１４から第２記憶装置のRAM ７３に読み取られる。そして、同じく、ステップ224 において、その暗号化登録指紋画像データは、第２記憶装置のRAM ７３に第１記憶装置のRAM ７２から転送された暗号解読キーデータに基づいて、解読され、復号化された登録指紋画像データに変換され、第２記憶装置のRAM ７３の所定領域に記憶される。

次に、ステップ226 で、ステップ208 と同様にして、画像処理プロセッサ７１が起動され、第２記憶装置のRAM ７３の所定領域に記憶された登録指紋画像データと、同じく、第２記憶装置のRAM ７３の所定領域に記憶された入力指紋画像データとの照合演算が実行される。

そして、ステップ228 で、ステップ210 と同様にして、２つの指紋画像データが一致するか否かが判定され、一致すれば、ステップ212 以下の使用者登録のステップが実行される。

又、ステップ220 で、入力ＩＤコードが通常管理者のＩＤコードと一致しないと判定された場合や、ステップ210 又はステップ228 で、２つの入力指紋画像データと登録指紋画像データとが不一致と判定された場合には、コンピュータ装置の現在の操作者は最優先管理者でも通常管理者でもないので、使用者登録を行うことが出来ず、ステップ230 でその旨の表示がCRT ディスプレイ３０に表示され、ステップ210 へ戻る。

次に、ステップ212 以下の使用者登録のステップについて説明する。

上記のようにして使用者登録が許可される、ステップ212 において、これから登録する者のＩＤコードと、登録する者が通常管理者か他の一般の使用者かを区別する管理者識別データがキーボード９０から入力される。そのＩＤコードと管理者識別データは、画像処理プロセッサ７１を介して第１記憶装置のRAM ７２の所定領域に記憶される。

次に、ステップ214 で、指紋画像入力装置５０及び画像処理プロセッサ７１が起動され、指紋画像が読み取られ、２値化された指紋画像データが第２記憶装置のRAM ７３に記憶される。次に、ステップ216 において、その指紋画像データが、ＩＤコードに対応した暗号変換テーブルに従って、暗号化される。次に、その暗号化された暗号化登録指紋画像データは、ステップ218 で、フロッピィディスク１４のＩＤコードに対応して所定領域に記憶される。

このようにして、通常管理者及びその他の使用者の指紋画像データは暗号化された後に、フロッピィディスク１４に記憶される。

(3) コンピュータ装置の使用時の使用者確認

コンピュータ装置は、上記のようにして登録された最優先管理者、通常管理者及び他の使用者以外には使用が許可されない。

コンピュータ装置の使用を許可するか否かの処理は、第６図に示すフローチャートに従って実行される。

ステップ300 ～ステップ310 は、使用者が最優先管理者である場合の本人確認の処理ステップであり、第５図で説明した使用者登録時に実行される本人確認の処理ステップ200 ～ステップ308 と全く同様である。

又、ステップ320 ～ステップ330 は、使用者が登録された通常管理者か他の使用者である場合の本人確認の処理ステップであり、第５図で説明した使用者登録時に実行される本人確認の処理ステップ220 ～ステップ230 に対応する。ただ、使用時の本人確認は、登録された通常管理者及び他の登録された使用者（以下、この２者を「通常登録者」という）に対して確認が実行される。

そして、本人確認がなされた場合には、ステップ312へ移行して、本人確認の情報をＯＳに伝達して、本プログラムを終了する。

その後、ＯＳは、本人確認があった場合にのみ、他のアプリケーションプログラム等の実行を許可する。

上記実施例では、最優先管理者の登録指紋画像データを第１記憶装置のRAM ７２に記憶し、通常登録者の登録指紋画像データを暗号化してフロッピィディスク１４に記憶するようにしている。従って、最優先管理者は、フロッピィディスクが異なっても、本コンピュータ装置の使用が許可される。それに対し、通常登録者は、フロッピィディスク毎に記憶するので、使用するフロッピィディスク（使用システムやアプリケーションプログラム）が異なれば、コンピュータ装置を使用することが禁止される。このように、使用者管理に柔軟性を持たせることができる。

尚、上記実施例において、暗号化手段の機能はステップ216で実現され、復号化手段の機能はステップ224又はステップ324で実現され、これらのハードウエアは、主として、CPU 12、RAM 16で具体化されている。又、照合手段の機能はステップ226、228又はステップ324、326及び画像処理プロセッサで実現され、そのハードウエアは主として、CPU 12、RAM 16、画像処理プロセッサ７１で具体化されている。又、データ転送手段の機能はステップ202又はステップ302及び画像処理プロセッサで実現され、そのハードウエアは主として画像処理プロセッサで具体化されている。

又、上記実施例では、外部記憶装置としてフロッピィディスク装置を用いているが、固定ディスク装置を有しているコンピュータ装置であれば、その固定ディスクに通常登録者の暗号化登録指紋画像データを記憶するようにしても良い。

又、コンピュータ装置は、外部記憶装置に対してアクセス可能な汎用又は専用用途を有する広い意味の装置を指し、ホストコンピュータの端末装置、単独で動作するコンピュータ装置等の汎用装置の他、情報検索装置、図面作成装置、回路設計装置等の専用用途のコンピュータ装置も含まれる。

又、暗号化の手法は、乱数コードテーブルによるデータ変換の他、登録指紋画像データをランレングス変換によりデータ圧縮するに際し、ラン長を使用者のＩＤコードに対応して可変することで、指紋画像データを暗号化することができる。

又、データ圧縮の際に、任意の場所に冗長な情報を挿入することで、更に、解読を困難とすることも可能である。

【発明の効果】

本発明では、使用者の指紋画像データを暗号化して外部記憶装置に記憶させ、復号のための解読鍵データはコンピュータ装置からは、直接、アクセスできない第１記憶装置に記憶させて、照合時にのみ、コンピュータ装置からアクセス可能な第２記憶装置にそのデータを転送するようにしているので、指紋照合装置等の記憶容量を増加させることなく、機密を保持した多数の使用者の登録が可能となる。

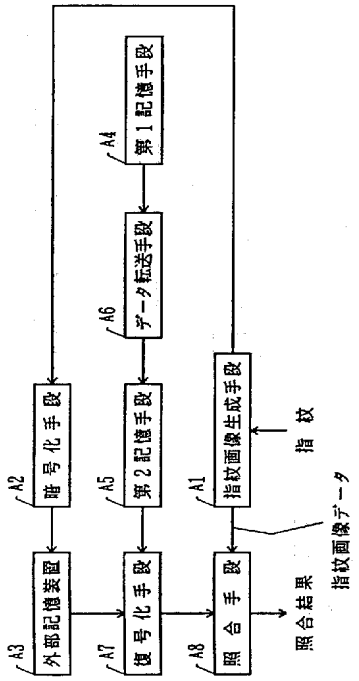
4. 図面の簡単な説明

第１図は本発明の概念を示したブロック図、第２図は本発明の具体的な一実施例に係る使用者確認装置の構成を示した斜視図、第３図は同実施例装置の構成を示したブロック図、第４図は最優先管理者の登録のCPU による処理手順を示したフローチャート、第５図は使用者登録のCPU による処理手順を示したフローチャート、第６図は使用時の使用者確認のCPU による処理手順を示したフローチャートである。

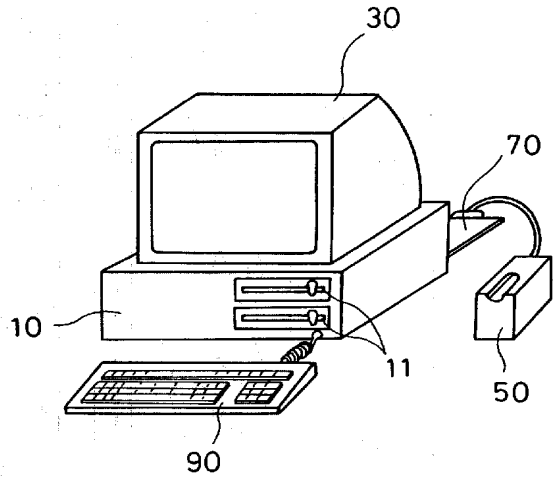
１０……コンピュータ装置本体
１１……フロッピィディスク装置
５０……指紋画像入力装置
７０……画像処理装置

特許出願人　　日本電装株式会社
代理人　　弁理士　藤谷　修

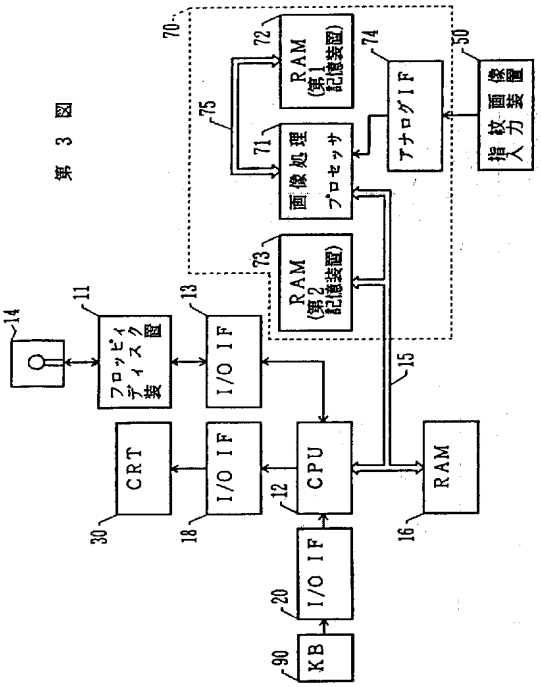
第１図



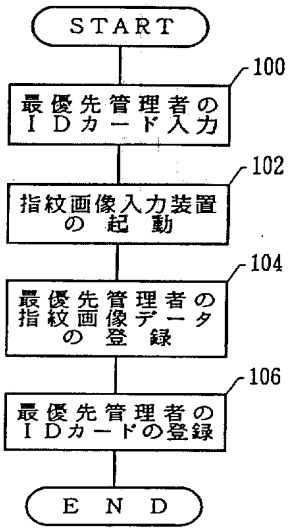
第２図



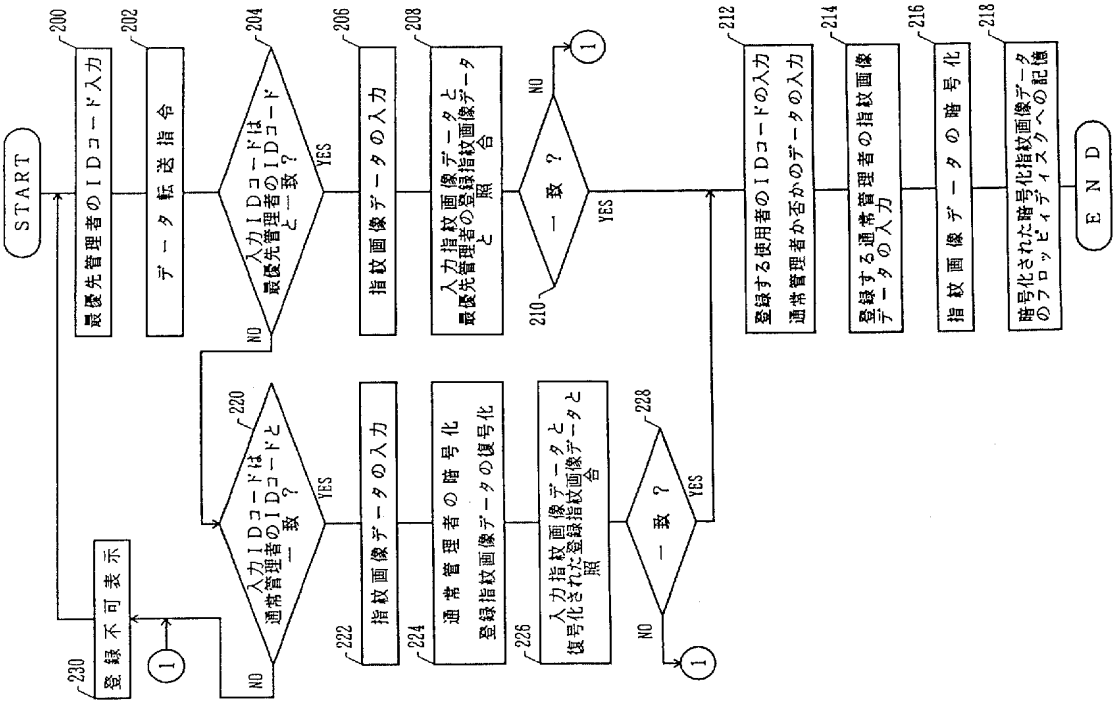
第３図



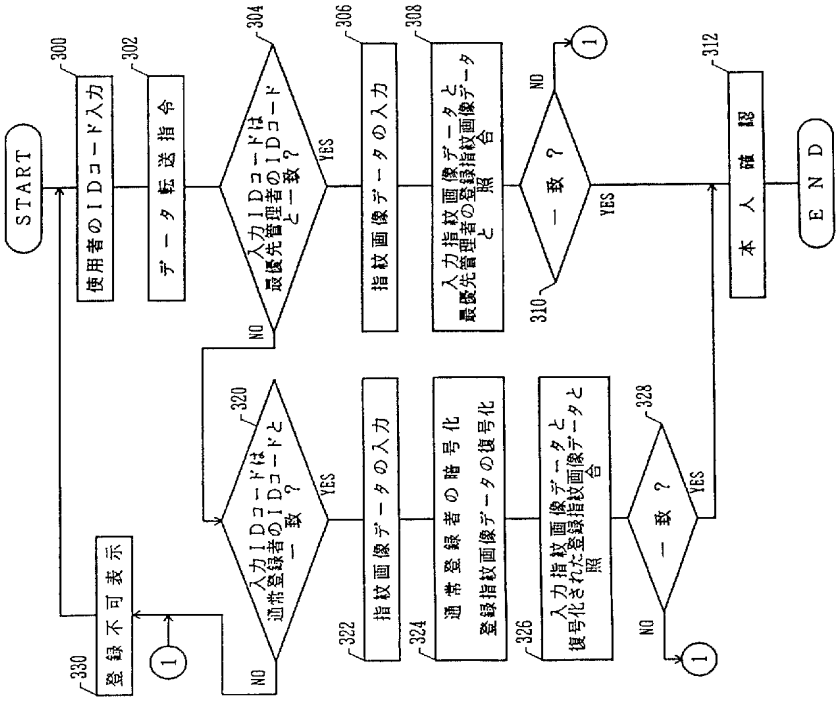
第４図



第 5 図


START
200
最優先管理者のＩＤコード入力
202
データ転送指令
204
入力ＩＤコードは最優先管理者のＩＤコードと一致？
NO
YES
206
指紋画像データの入力
208
入力指紋画像データと最優先管理者の登録指紋画像データと照合
210
一致？
NO
YES
212
登録する使用者のＩＤコードの入力
通常管理者か否かのデータの入力
214
登録する通常管理者の指紋画像データの入力
216
指紋画像データの暗号化
218
暗号化された暗号化指紋画像データのフロッピィディスクへの記憶
END
220
入力ＩＤコードは通常管理者のＩＤコードと一致？
NO
YES
222
指紋画像データの入力
224
通常管理者の暗号化登録指紋画像データの復号化
226
入力指紋画像データと復号化された登録指紋画像データと照合
228
一致？
NO
YES
230
登録不可表示
①

第 6 図


START
300
使用者のＩＤコード入力
302
データ転送指令
304
入力ＩＤコードは最優先管理者のＩＤコードと一致？
NO
YES
306
指紋画像データの入力
308
入力指紋画像データと最優先管理者の登録指紋画像データと照合
310
一致？
NO
YES
312
本人確認
END
320
入力ＩＤコードは通常登録者のＩＤコードと一致？
NO
YES
322
指紋画像データの入力
324
通常登録者の暗号化登録指紋画像データの復号化
326
入力指紋画像データと復号化された登録指紋画像データと照合
328
一致？
NO
YES
330
登録不可表示
①